NAVAL WAR COLLEGE
Newport, R.I.

Planning Information Operations to Enable Assured Access

by

James L. Gray, Jr.
LCDR, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Maritime Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: J L Gray
05 February 2001

Faculty Advisor: ______________________
Prof. Roger Barnett

10

REPORT DOCUMENTATION PAGE

1. **Report Security Classification:** UNCLASSIFIED

2. **Security Classification Authority:**

3. **Declassification/Downgrading Schedule:**

4. **Distribution/Availability of Report:** DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. **Name of Performing Organization:** JOINT MILITARY OPERATIONS DEPARTMENT

6. **Office Symbol:** C

7. **Address:** NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. **Title** (Include Security Classification):
PLANNING INFORMATION OPERATIONS TO ENABLE ASSURED ACCESS (U)

9. **Personal Authors:** LCDR James L. Gray, Jr., USN

10. **Type of Report:** FINAL

11. **Date of Report:** 05 February 2001

12. **Page Count:** 20

12A **Paper Advisor (if any): Prof. Roger Barnett**

13. **Supplementary Notation:** A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. **Ten key words that relate to your paper:**
Information Operations, IO, Information Warfare, IW, Assured Access, planning, OPLAN, targeting, NWDC, Operational Functions

15. **Abstract:**

The end of the Cold War brought about an exponential increase in the quantity and quality of long-range precision weapons available to Third World countries. This trend is going to make it more and more risky for U.S. forces to project power against a country who possess these weapons. The solution to this problem is currently being called "Assured Access" and is a very complicated subject. Information Warfare (IW) offers the potential to help solve the assured access problem by minimizing risk to forces operating within weapons range of a hostile country. The problem is that current plans are not being revised to fully integrate IW with other warfare disciplines.

One method to focus this effort is to analyze IW functions in terms of operational functions. This allows for the analysis of IW mission enablers and detractors. The logical follow through would then be to develop workarounds so that incorporating IW results in an overall more effective plan. This same analysis can be used by the tactical commander to evaluate changing situations and alternate courses of action.

It is time to start integrated planning and to exercise this capability with the fleet.

16. Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**

17. **Abstract Security Classification:** UNCLASSIFIED

18. **Name of Responsible Individual:** CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. **Telephone:** 841-6461

20. **Office Symbol:** C

Security Classification of This Page **Unclassified**

<u>Abstract</u>

PLANNING INFORMATION OPERATIONS TO ENABLE ASSURED ACCESS

The end of the Cold War brought about an exponential increase in the quantity and quality of long-range precision weapons available to Third World countries. This trend is going to make it more and more risky for U.S. forces to project power against a country who possess these weapons. The solution to this problem is currently being called "Assured Access" and is a very complicated subject. Information Warfare (IW) offers the potential to help solve the assured access problem by minimizing risk to forces operating within weapons range of a hostile country. The problem is that current plans are not being revised to fully integrate IW with other warfare disciplines.

One method to focus this effort is to analyze IW functions in terms of operational functions. This allows for the analysis of IW mission enablers and detractors. The logical follow through would then be to develop workarounds so that incorporating IW results in an overall more effective plan. This same analysis can be used by the tactical commander to evaluate changing situations and alternate courses of action.

It is time to start integrated planning and to exercise this capability with the fleet.

Since the end of the Cold War, many countries throughout the World have pronounced their intention to exert influence locally and have postured weapons to control areas adjacent to their borders. This is driven, in part, by the increasing ease of buying and producing weapons. In addition, many countries are actively developing the doctrine and proficiency required to effectively employ these weapons. A few examples include the numerous test firings of ballistic missiles by India and Pakistan, the use of anti-ship cruise missiles during Iranian fleet training, and the purchase of diesel submarines by many naval countries. If the U.S. became embroiled in a conflict with one of these countries, the adversary could pose a difficult challenge if the U.S. needed to operate within the adversary's weapons envelope to project power. The solution to this access problem is complex and has great ramifications. But like the proverbial elephant, it must be eaten one bite at a time and this paper discusses how Information Operations (IO) can be planned to facilitate assured access. Keep in mind through the reading of the paper that IO is only one piece and if you want to restore the whole elephant, you have to put the pieces back in just the right place. Moreover, the arguments will be limited to a discussion in terms of maritime operations only. However, the principles can be equally applied to a ground force establishing a base of operations in a contested area, an air force operating in enemy controlled space, or any other scenario where access is required but being denied by the adversary.

Specifically, this paper will discuss what the operational commander can do right now to plan for operations that require access to a denied area. Although some believe that a new technological solution might be developed that fundamentally changes the nature of warfare, it has yet to come to fruition. However, IO doctrine is still a relatively new frontier and there is significant potential to improve warfighting capabilities just by more effectively utilizing the hardware already in existence. This paper will further that process.

In order to start from a common point, this paper makes some assumptions. First, there is an ongoing conflict with an adversary who has the means, skill, and will to put opposing forces at risk within an area adjacent to their boundary. Second, in order to accomplish the mission, friendly forces must conduct operations within the area of risk. This last assumption is going to be contested by some who argue that the U.S. could use long-range weapons and just stay beyond the reach of the adversary's weapons. The answer to this debate is beyond the scope of this paper; however, many have already argued that in future conflict the U.S. will have to operate within the enemy's weapons range. Former Chief of Naval Operations, Admiral Jay Johnson argued that countering a potential adversary's area denial efforts "will become the single most crucial element in projecting and sustaining U.S. military power where it is needed."[1] Professor Thomas Mahnken postulates that the proliferation of precision weapons and advanced sensors will allow a foe to project power far enough from the coast that it will undermine the capability of the U.S. to project power.[2]

There is a common misperception that IO is limited to Computer Network Attack (CNA) and Computer Network Defense (CND). In fact, the major functional areas of IO include: "OPSEC [operational security], PSYOP [psychological operations], military deception, EW [electronic warfare], physical attack/destruction… public affairs (PA) and

[1] Admiral Jay Johnson, "Anytime, Anywhere: A Navy for the 21st Century", U.S. Naval Institute Proceedings, (November 1997): 49.

[2] Tomas G. Mahnken, "Deny U.S. Access?", U.S. Naval Institute Proceedings, (September 1998): 36-37.

civil affairs (CA)…"[3] CNA and CND are techniques applied in IO. A subset of IO is Information Warfare (IW), which is the use of IO during times of crisis and conflict. This paper will discuss how all of the parts of IW can be leveraged to gain assured access. For a list of acronyms and definitions refer to Joint Pub 3-13, Joint Doctrine for Information Operations.

The Challenge

To date, the U.S. and its allies have yet to include IO as part of the integrated planning for an operation. Most recently during the conflict in Kosovo, the IW planning was started significantly after the rest of the military planning and was conducted in semi-isolation. Secretary of Defense William Cohen and Chairman of the Joint Chiefs of Staff General Henry Shelton testified in front of the Senate Armed Services Committee on 14 October 1999 that "the conduct of an integrated information operations campaign was delayed by the lack of both advance planning and strategic guidance defining key objectives."[4] This is despite a comment by General Shelton in March 1999 that "information operations and information superiority are at the core of military innovation and our vision for the future of joint warfare… The capability to penetrate, manipulate, and deny an adversary's battlespace awareness is of utmost importance."[5] This seeming disconnect can probably best be explained by the relative infancy of IO. The initial IO doctrine, JP 3-13, was published less than six months prior to the start of operation Allied Force. Even General Wesley Clark, Supreme Allied Commander Europe during Allied Force, more recently

[3] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), I-9-10.

[4] Timothy L. Thomas, "Kosovo and the Current Myth of Information Superiority", Parameters, 30 (Spring 2000): 13.

[5] Ibid., 13.

speculated that the aerial assault might not have been required if other means had been employed such as "methods to isolate Milosevic and his political parties electronically."[6] Senior leadership has identified IO as an area of great potential.

Even though IO is getting lip service from Department of Defense (DOD) leadership, there is still some question about how well IO is being integrated into operations. In a DOD after action report to Congress about Kosovo, IO received three sentences worth of attention. DOD told congress "... the conduct of integrating information operations was hampered by the lack of advance planning and necessary strategic guidance to define key objectives. The Department will address this problem by developing the needed plans and testing them in exercises."[7] This guidance is not being executed by all of the Combatant Commanders, who are responsible for maintaining plans and in part for exercising forces.[8] This problem is not because there is a lack of ideas. The services have been developing doctrine, tactics, techniques, and procedures for over 8 years. In respect to the Air Force: "The service officially established IW as a priority in 1993, shortly after the Department of Defense developed its own IW policy."[9] Although the Air Force got a head start, all of the other services are fully on the bandwagon and moving at full speed. Part of the reason for this disconnect at the CINC level is a lack of understanding how IO integrates with the more

[6] Ibid., 14.

[7] Department of Defense, Report to Congress: Kosovo/Operation Allied Force After Action Report, (31 January 2000): 99.

[8] This is based on personal experience at U.S. Central Command. I was involved in the rewrite of one OPLAN and 2 CONPLANS in 1999-2000. Although I did not have direct responsibility for planning IO, I was involved in the rest of the J-3 revisions. There may have been revision to IO sections of the plan but they remained stovepiped and were not integrated with the rest of the plan. Exercise Bright Star in 1999, one of CENTCOMS largest exercises, in no way exercised IO.

[9] Major Gary Pounder, USAF, "Opportunity Lost: Public Affairs, Information Operations, and the Air War against Serbia", Aerospace Power Journal, (Summer 2000): 59.

traditional elements of the military. Presented later in this paper is a possible approach to this problem.

In time of crisis, when it has been determined that military force is required, it is the job of the operational commander to project power at the place and time of his choosing. This implies that he will mass force and economically employ it in a way that most directly achieves the objective. This is part of what Joint Vision 2020 (JV 2020) calls Full Spectrum Dominance and more specifically describes it as:

> "...the ability of US forces ... to defeat any adversary and control any situation across the full range of military operations. ...The label Full Spectrum Dominance implies that US forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all domains – space, sea, land, air, and information. Additionally, given the global nature of U.S. interests and obligations, it must maintain its overseas presence forces and the ability to rapidly project power worldwide in order to achieve full spectrum dominance."[10]

The question is how to get forces where they are needed, at the correct time, and with the least amount of risk.

Risk is a noteworthy topic because the most immediate benefits from IO are potentially in the area of risk reduction. Some might argue that if the objective was worthy enough, power could be projected in the style of D-day at Normandy where sheer numbers were used to overcome overwhelming opposing force. However, the current trend is to get involved in conflicts that are not of vital national interest. Therefore it is unlikely to see such an operation with the risks and costs similar to the landing at Normandy. In addition, the time required to mount such a large-scale invasion would allow the enemy to generate force, which would result in raising the cost for friendly forces to project power. This is why JV

[10] Chairman of the Joint Chiefs of Staff, Joint Vision 2020; America's Military: Preparing for Tomorrow (Washington, DC: n.d.), 6.

2020 calls for prompt action. Besides, it should not be lost that the landing at Normandy was preceded by a huge military deception effort, which most certainly reduced the risk. In any event, minimizing risk has become a heavily weighted factor in the planning process.

The planner will have to prepare for the many types of anti-access strategies that the adversary is likely to employ. Although it is not possible to predict all of the potential threats, they can be discussed in terms of today's technology. Most enemy strategies are likely to employ weapons that will put friendly forces at risk in the vicinity of hostile coastlines. This might seem obvious, but it has important implications since it defines the space within which friendly forces can freely operate as opposed to where they will be at risk. Examples of the weapons friendly forces will face include, but are not limited to, "quiet submarines, mines, tactical ballistic missiles, anti-ship cruise missiles, information warfare technology, and chemical and biological weapons of mass destruction."[11]

All of these weapons require some degree of targeting to be effective. Even mines need to be targeted by placing them where they would have the most effect against the enemy while preventing fratricide. Therefore a critical link in the weapons delivery chain is the enemy's ability to target and where IW has the most potential. If friendly forces can break that link using IW, then they have significantly reduced the risk to their forces. Of course, if this fails and a weapon is accurately targeted and launched, then IW should be able to provide that information and a means to counter the incoming weapon.

The Solution

The best way to frame this is in terms of Colonel John Boyd's theory of the OODA loop: Observe, Orient, Decide, Act. IW could and should target all four aspects of this cycle;

[11] "Submarine Themes: Denied Areas", Unites State Navy Submarine Centennial, <http://www.chinfo.navy.mil/navpalib/ships/submarines/centennial/denied.html>, [25 January 2001].

however, the start of the loop occurs in the Observe phase, therefore effects there will ripple throughout. Management of an enemy's observations can be broken into two major categories: either deny information or manipulate it. The choice of method will depend on many factors, which include, but are not limited to: friendly capabilities, current objectives, and enemy disposition. The OPLAN should allow for switching between methods as well as using both simultaneously.

Targeting is not a trivial issue and is analogous to the 'orient' phase of the OODA loop. It requires the enemy to locate and classify opposing forces in a precise, timely manner; and then relay that information, along with launch orders, to the weapons platform. The location error of friendly forces is a function of navigational, guidance, and target location errors and will grow as a function of time[12]. There is much here that can be affected. For example, if the targeting platform had an undetected 2nm navigation error or if the missile gyro could be offset by five degrees it could be enough to cause a miss. Any technique that can affect these factors or insert a delay between targeting and launch will mitigate risk to friendly forces.

The last two phases of the OODA loop equate to C2 and weapons employment. The operational commander should build a plan that addresses all of these while minimizing interference with other aspects of the operation.

Operational Commander's Perspective

[12] This relationship was provided by Prof. Roger Barnett from the Naval War College via email. Prof. Barnett has done extensive research in this area.

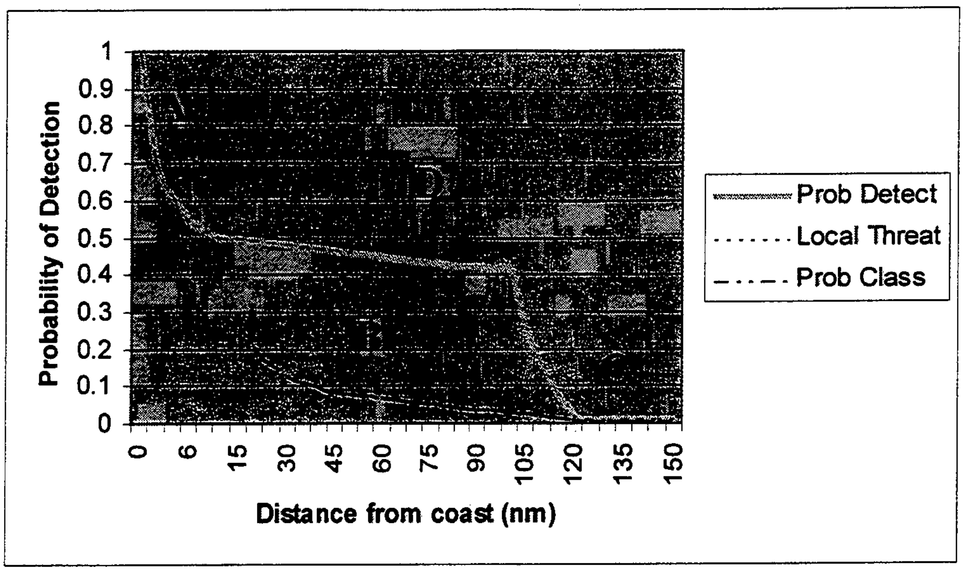

Figure 1. Probability of Detection vs. Range from Coast

In order to mass forces at a decisive point, the operational commander must develop a scheme of maneuver that aspires to bring forces to that point unchallenged and ideally, undetected. The first step in this analysis is to determine the enemy's threshold of detection and classification. Figure 1 is a representation of fictitious enemy detection and classification ranges and is for illustrative purposes only. Region A represents an area of high risk of detection and classification. Region B represents an area of high probability of detection, but relatively low probability of classification. In region C there is very little risk of detection or classification. Region D represents a local area of increased enemy detection capabilities due to a mobile sensor such as an aircraft or ship. This region will continually change shape and size based on the locations of the mobile sensors. The operational commander will probably have a good idea about where regions A through C are and can set his scheme of maneuver accordingly. If the operational commander could operate completely within region C, then anti-access would be a non-issue. However, region D will be time and space dependent and therefore the operational commander will have to express

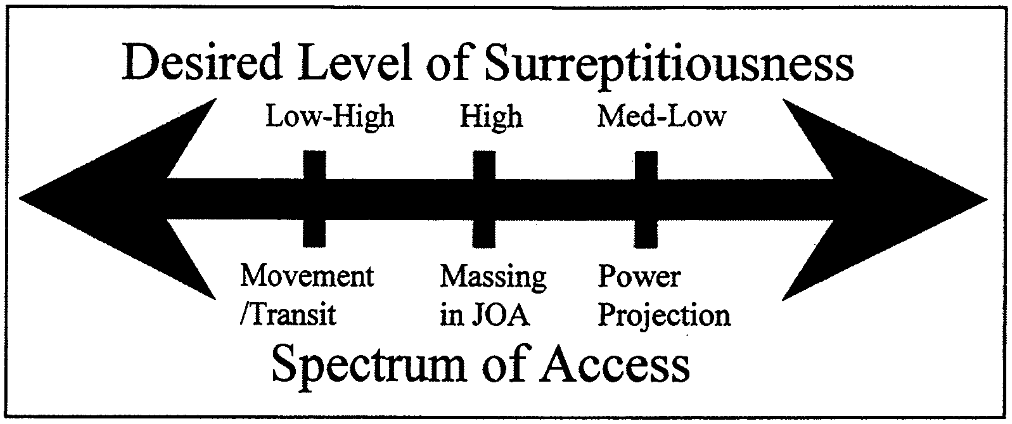

Figure 2. Operating Spectrum

his intentions with respect to this region so that the tactical commander can take appropriate action in a timely manner. Possible action will span the spectrum from passively monitoring the mobile sensor to destroying it. To project power friendly forces will probably be faced with operating in all of the regions.

Now that the operational commander understands the space within which he can potentially operate, he must decide where on the spectrum of access he wishes to operate as a function of time and location (figure 2). This spectrum can be used to express how high of a priority to place on remaining undetected during different phases of an operation. It is important to note that a commander should consider the desire to move both ways along the spectrum based on timing or phasing of the operation. As an example, while transiting across an ocean the commander must weigh the deterrent effect of ensuring the enemy knows his progress against the element of surprise. When the friendly force is constrained to move through an area within detection range of a state sympathetic to the enemy, then the commander might choose a high degree of surreptitiousness to prevent expanding the conflict to this country. Once forces are massed and the desire is to project power, the restraints imposed by remaining undetected could put the ensuing offensive actions at risk and therefore would not be desirable. To effectively control this spectrum, the operational commander must make it an integral part of his plan. He must design sequels and branches to allow for flexibility.

The spectrum in figure 2 could be discussed in terms of moving from defense to offense. The idea here is that on defense every measure is taken to remain undetected while on offense some of those measures could hinder operations and so therefore they are relaxed. This is a suitable model as long as it is realized that it describes a spectrum with an infinite number of perturbations.

To better understand how the operational commander should integrate IW into an OPLAN, it is appropriate to dissect IW into the functional areas described earlier (OPSEC, PSYOPS, EW, etc…). It is important to remember that for analytical purposes these parts are treated separately here; however, in the real World they influence each other and other aspects of the mission. In every case, while pursuing a particular IO functional area, secondary effects can run counter to the overall mission objective. One way to evaluate this is to break each IW function into the operational functions[13] that it will affect. Once it is determined which operational functions will be negatively affected, the overall plan can be modified to mitigate the impacts. The overall analysis of enablers, detractors, and workarounds will expose the best IW course of action to incorporate into the overall plan.

Referring back to Figure 2, remember that the desired level of surreptitiousness will change through the phasing of the operation. This will result in IW having a varied level of impact on the operational functions. Therefore, the analysis of the above paragraph should be repeated for each phase of the mission where the required level of surreptitiousness

[13] Operational functions include Command and Control, Operational Intelligence, Movement and Maneuver, Logistics, Operational Fires, and Operational Protection.

changes. There may be times when a second order effect, or detractor, is unacceptable and other times when it will have little impact.

To better illustrate this process, an example follows. Table 1 is provided up front as a summary of the analysis. This 'stop light' chart is a useful tool not only during the planning phase but also during execution as a reminder of overall expected effects. Remember that this is for illustrative purposes only and that the way in which IW impacts real World ops will be mission and case specific.

	C2	Intel	M & M	Log	OP Fires	OP Prot
OPSEC	⇩	⇩	⬆	⇩	⇔	⬆
PSYOPS	⇔	⬆	⬆	⇔	⬆	⇩
MIL Deception	⬆	⬆	⇩	⇩	⇔	⬆
EW	⇔	⇩	⇔	⇔	⬆	⬆
Physical Attack	⇔	⇔	⬆	⇩	⬆	⬆

Table 1. IW effects analysis summary

OPSEC can be a double-edged sword that tends to complicate planning and execution. Too much OPSEC can hinder the flow of ideas and slow down speed of command. However, as discussed earlier, one of the key elements to assured access is the ability to protect friendly forces by denying the enemy the ability to target. OPSEC plays a central role in that it eliminates, or at least reduces, cueing and locating information. A tight OPSEC posture will probably be required if friendly forces are to remain undetected. The detractors will occur in the areas of C2, intelligence and logistics; however, some thoughtful planning can mitigate the impact. Command and control (C2) relies heavily on radio waves, which are a primary source of counter-detection. According to a recent study, "Electromagnetic (EM) emissions, radar cross section (RCS), and underwater acoustics (i.e., radiated noise) are the most important signatures to a threat because they have the potential of being exploited across the entire range spectrum of an attack."[14] A strict OPSEC posture will severely limit EM transmissions. This can be overcome to some extent if the operational commander plans to use communications links that have a low probability of being intercepted (LPI) such as: low power, line-of-sight links and metered use of commercial communications. However, all of these methods might restrict bandwidth to significantly less than desired; therefore, to make these alternative methods work, they need to be incorporated into doctrine and practiced so that operators can quickly adjust to these restrictions.

Organic intelligence will be limited due to the detection risk to the sources. Examples include IMINT and SIGINT from organic aircraft and radar surveillance. The ability to query national and supporting assets could sometimes be limited if there was a risk that even the LPI communications could be intercepted. During these periods the intelligence support would be unresponsive to local conditions unless a detailed intelligence support plan is developed in advance that is keyed to events or phasing and that pushes information to the force. Examples of some sources that would not compromise OPSEC include national assets, Air Force collection assets such as the RC-135, Special Forces, and information gathered from computer intrusion. A well-crafted plan would provide useful and timely information and could be easily modified with very little bandwidth.

Logistics could be degraded if emergent needs could not be transmitted because of reduced bandwidth. In addition, the plan might call for forces to bypass traditional maintenance ports to maintain secrecy about their location. Two factors might be planned to

[14] Costa Vatikiotis and Thomas Taylor (Center for Naval Analysis), Signature-Management Alternatives for Improving Future Aircraft-Carrier Survivability (Alexandria, VA:1992), A-1.

mitigate this problem. The first is to use speed to minimize movement time and thus allow less time for Murphy's Law to take effect (i.e. equipment to break) . The second is to plan resupply ships to meet the force along the way. Any requirements that could not be met by a supply ship could be relayed securely by that ship and made available at the next rendezvous.

PSYOPS can be a tremendous enabler by affecting the will of the adversary to engage in hostilities. Ideally PSYOPS are targeted at the political leadership, but in reality troops on the field are often the target. The detractor is that by targeting the troops that pose the greatest threat to friendly forces, the PSYOPS effort could be analyzed by the enemy and thus reveal a pattern that would divulge the intended track of friendly forces. The workaround involves inserting a degree of randomness into the PSYOPS targets to ensure that no trend can be established.

Military Deception enables access by causing the enemy to look and commit forces to areas where friendly forces are not located. In an area with relatively small operating space, friendly forces will be restricted in their choice of maneuver room and Lines of Communication (LOCs) since they will have to avoid the areas that are the subject of the deception effort. In this case an inverse relationship is formed between maneuver and deception. The proper balance must be struck to maximize the chances of mission success.

Certain aspects of Electronic Warfare, such as jamming, could interfere with intelligence vital to the completion of the mission or safety of friendly forces. For instance, destruction of a C2 node that was being monitored and was providing critical information about enemy intentions might do more harm to friendly information superiority than to hurt the enemy C2. The details of the deconfliction have to be worked out at the tactical level, but the operational commander should give guidance either in the form of intent or priorities to focus the team on this issue.

A physical target of the operation might be to destroy computers that operate the railroad switching system to hinder the enemy's ability to resupply. A follow-on phase of the friendly operation is a fast, deep penetration into the interior that is supposed to rely on the rail system for logistics. A better alternative might have been to disable the rail system such that it could be repaired when needed or to bring a long a replacement system that could be installed when needed.

Through the method of analysis such as presented here, all of the 'pieces' of IW that can potentially enable an operation can be examined for benefits and detractors to the overall mission. Solutions to the detractors can be evaluated with respect to the overall mission and incorporated if shown to have merit. Several courses of action can be evaluated by this method and compared.

The Stake in the Road

The U.S. Navy is already trying to answer the question of how best it integrate IW into an operation requiring power projection into a denied area. The main effort is occurring at the Navy Warfare Development Center (NWDC) where they are currently working on a series of discussions and games called Concepts for the Navy After Next[15] (CNAN). They are taking a phased approach by starting with discussions, moving to tabletop war games, then to computer simulated war games, and finally experimentation in the fleet. Currently they are in the computer simulation phase. According to Mr. Wayne Smith from NWDC who is working on the CNAN project, "the last game did not go very well with deception

[15] Naval Warfare Development Center, The Information Operations Game: CNAN Loop 4 (Newport, R.I.: November 2000), 4.

mainly because the IO planning efforts were not well integrated into the overall plan."[16] The plan now is to figure out how best to integrate and deconflict IO with an OPLAN and then game it again to determine the results.

It is curious that the term IO has officially been in existence for eight years and the Navy has not at least experimented with some aspects of it out in the fleet. Besides the phased approach described earlier, Mr. Joe Vann of NWDC offers some more detailed reasons for the probable causes: "Deception is hard to exercise for several reasons: 1) it is disruptive to operations; 2) reception by the fleet could expose weaknesses; 3) there is a possibility that the deception could go so well that the opposing force could spend the whole exercise chasing ghosts. You would then have to restart the exercise for the purpose of allowing the fleet elements to exercise tactical mission capabilities. This would mean a rather large expenditure for the exercise with marginal returns in the operational aggregate; lastly, 4) it is difficult to exercise deception objectives without compromising real potential deception scenarios that could actually be used during time of war."[17] Even through USCINCPAC exercise Tempo Brave 96 was designed in part to test IW, it was concluded that in fact some of the above reasons contributed to the complete failure to implement and test IW[18]. Though Mr. Vann's analysis is a very reasonable approach, the Navy routinely conducts large, complicated exercises in preparation for deploying every carrier battlegroup and each of these could include some aspect of IO planning with very little impact. Each one of these is an opportunity missed.

[16] Mr. Wayne Smith, Naval Warfare Development Center, interview by author, 29 January 2001, Naval Warfare Development Center.

[17] Mr. Joe Vann, Naval Warfare Development Center, interview by author, 29 January 2001, Naval Warfare Development Center.

[18] Gary A. Federici and Thomas P.M. Barnett (Center for Naval Analysis), Information Warfare Training in Tempo Brave 96: The Dog That Did Not Bark (Alexandria, VA: 1997), 17.

Conclusion

Although many of the pieces of IO have been around many years, IO as a doctrine and integrated part of an OPLAN is still in the infancy stage. There is a chance that someday war can be fought completely in the information realm, but for the near future it still needs to be integrated into OPLANS to support the more conventional forms of power. Like a puzzle piece, the relationship to the 'big picture' must be established so that IO supports without detracting from the overall mission. Although there are numerous ways to do this analysis, the one presented in this paper is a possible approach. The advantage being that it falls in line with the traditional way to analyze a mission through operational functions. Planners who already understand and routinely use operational functions as a framework for mission analysis and planning can easily adopt this approach.

The Navy and the other Services are already well on the way to developing tactics, techniques and procedures to employ IO, but the shortfall now is the integration into the overall planning effort. It is not too early to start that integration process. What is required is a joint effort between the Combatant Commanders and the Services to work what is feasible today into the existing plans and a process to update the plans as IO matures. This should maximize the effectiveness of current plans within the realm of what is possible today and prevent them from becoming outdated as technology progresses.

Recommendations

1) The Navy should start looking for and exploiting opportunities to exercise IO planning and execution in the fleet.

2) A standardized method should be developed to integrate IO into an OPLAN and OPORD.

Bibliography

Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force." Naval War College Review (Spring 1998): 7-19.

Barnett, Roger W. Surface Ship Survivability Risk Management and Newwork Centric Warfare. Newport, R.I.: Center for Naval Warfare Studies, Naval War College, 1998.

Federici, Gary A. and Thomas P.M. Barnett. Information Warfare Training in Tempo Brave 96: The Dog That Did Not Bark CAB 96-105. Alexandria, VA: Center for Naval Analyses, March 1997.

Heaton, Richard. Information Warfare in Recent Naval and Joint Operations CRM 94-132. Alexandria, VA: Center for Naval Analyses, November 1994.

Johnson, Jay. "Anytime, Anywhere: A Navy for the 21st Century." U.S. Naval Institute Proceedings (November 1997): 48-50.

Knowles, John. "A Wider View and a Bigger Bite: EW in Information Operations." Journal of Electronic Defense (October 1997): 51-57.

Kurdys, Martin P. "Information Warfare (IW) and Command and Control Warfare (C2W) for the Naval Expeditionary Task Force Commander." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

Mahnken, Tomas G. "Deny U.S. Access?" U.S. Naval Institute Proceedings (September 1998): 36-39.

Mayo, Dick. "From the Sea… to Cyberspace." U.S. Naval Institute Proceedings (October 2000): 44-48.

Naval Warfare Development Center. The Information Operations Game: CNAN Loop 4. Newport, R.I.: November 2000.

"Navy Plans to Focus on Assured Access, Information Dominance in Next QDR." Defense Daily, 208. 30 October 2000. PROQUEST. Potomac, MD (25 January 2001). To find this article on PROQUEST, use the search string "ISSN (08890404) and assured access and qdr".

Nelson, Bradford K. "Applying the Principles of War in Information Operations." Military Review (September-November 1998): 31-35.

Nieusma, William J. "The Operational Implications of Assuring Access." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 2000.

Pounder, Gary. "Opportunity Lost: Public Affairs, Information Operations, and the Air War Against Serbia." Aerospace Power Journal (Summer 2000): 56-78.

Rathmell, Andrew. "Information operations – coming of age?" Jane's Intelligence Review (May 2000): 52-55.

Smith, Wayne, Naval Warfare Development Center. Interview by author, 29 January 2001. Naval Warfare Development Center, Newport, R.I. .

"Submarine Themes: Denied Areas." Unites State Navy Submarine Centennial. <http://www.chinfo.navy.mil/navpalib/ships/submarines/centennial/denied.html> [25 January 2001].

Swider, Gregory, Harry Schmalz, Richard Heaton, Lloyd Koenig, and Mein-Sieng Wei. Information Warfare/C2 Warfare: Summary Report CRM 95-10. Alexandria, VA: Center for Naval Analyses, March 1995.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." Parameters, 30 (Spring 2000): 13-29.

U.S. Chairman of the Joint Chiefs of Staff. Joint Vision 2020; America's Military: Preparing for Tomorrow. Washington, DC: n.d.

U.S. Department of Defense. Report to Congress: Kosovo/Operation Allied Force After Action Report. Washington, DC: 2000.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, DC: 9 October 1998.

U.S. Naval War College. "The Littoral and Information Warfare Conference." Conference Report, U.S. Naval War College, Newport, RI: 3 March 1995.

Vann, Joe, Naval Warfare Development Center. Interview by author, 29 January 2001. Naval Warfare Development Center, Newport, R.I. .

Vatikiotis, Costa S. and Thomas D. Taylor. Signature-Management Alternatives for Improving Future Aircraft-Carrier Survivability CRM 92-60. Alexandria, VA: Center for Naval Analyses, June 1992.

Wald, Bruce and Alan Berman. Information Operations and Information Warfare: N3/N5 Responsibilities and Opportunities CRM 97-60. Alexandria, VA: Center for Naval Analyses, June 1997.